Cyber Resiliency

Rapid Recovery from Malware, Ransomware, Wiperware

Peter D. Bille – Storage Solution Specialist
Pdbille@ibm.com

The question is not IF you will be attacked but WHEN

$53 Billion

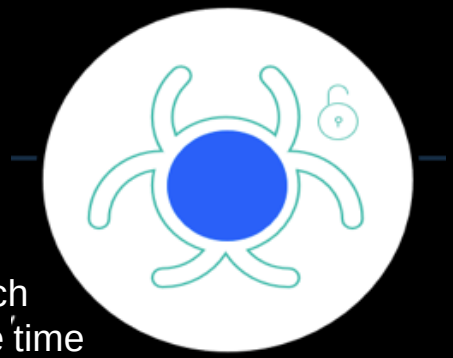
Predicted economic losses of the next global cyber attack

$5.2 Million

Average total cost of a data breach*

$8 Billion

Estimated global cost of WannaCry attack*



+ $137,000

Increase in data breach and incident response time costs due to remote work during COVID-19*

280 Days

Average amount of time hackers spend inside IT environments before discovery*

$230 Million

GDPR fine for one data breach*

- Cost of a Data Breach Report 2020, Ponemon Institute
- Riensirce news May 23 2017

HONDA

Honda Hackers May Have Used Tools Favored by Countries

The New York Times

REUTERS

'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals

GARMIN

The Garmin Hack Was a Warning

As ransomware groups turn their attention to bigger game, expect more high-profile targets to fall.

WIRED

The Register

UBS logic bomber jailed for eight years

Real-life BOFH ordered to pay $3.1m restitution

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

What is Cyber Resiliency?

According to NIST:

- The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
- Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment

What is Cyber Resiliency?

According to the European Central Bank (ECB):

- Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations ***quickly*** in case of a successful attack

What is Cyber Resiliency?

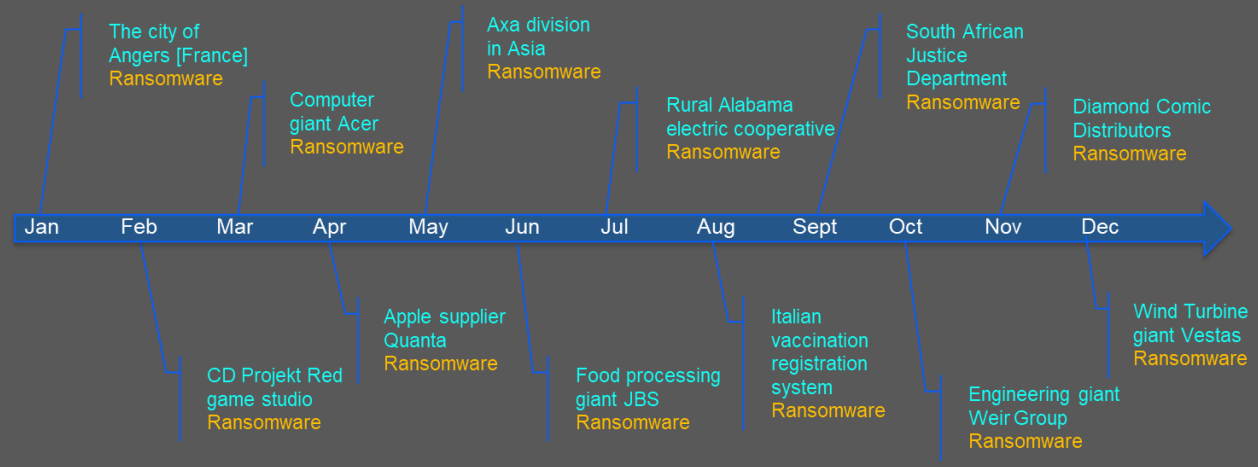
According to Wikipedia:

- **Cyber resilience** refers to an entity's ability to continuously deliver the intended outcome, despite cyber attacks.[1] Resilience to cyber attacks is essential to IT systems, critical infrastructure, business processes, organizations, societies, and nation-states. Adverse cyber events are those that negatively impact the availability, integrity, or confidentiality of networked IT systems and associated information and services.[2] These events may be intentional (e.g. cyber attack) or unintentional (e.g. failed software update) and caused by humans, nature, or a combination thereof.
- Unlike cyber security, which is designed to protect systems, networks and data from cyber crimes, cyber resilience is designed to prevent systems and networks from being derailed in the event that security is compromised.[3] Cyber security is effective without compromising the usability of systems and there is a robust continuity business plan to resume operations, if the cyber attack is successful.
- Cyber resilience helps businesses to recognize that hackers have the advantage of innovative tools, element of surprise, target and can be successful in their attempt. This concept helps business to prepare, prevent, respond and successfully recover to the intended secure state. This is a cultural shift as the organization sees security as a full-time job and embedded security best practices in day-to-day operations.[4] In comparison to cyber security, cyber resilience requires the business to think differently and be more agile on handling attacks.
- The objective of cyber resilience is to maintain the entity's ability to deliver the intended outcome continuously at all times.[5] This means doing so even when regular delivery mechanisms have failed, such as during a crisis or after a security breach. The concept also includes the ability to restore or recover regular delivery mechanisms after such events, as well as the ability to continuously change or modify these delivery mechanisms, if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms

The NIST Security Framework

Why Cyber Resiliency is important

2021 headlines in review



23 days

Average recovery after a ransomware attack

$5.2m

Average cost of Ransomware

83%

of Ransomware Victims Pay Their Attackers

5

Unexpected ransomware costs CFOs must account for:

1. Higher Borrowing Costs
2. Higher Insurance Premiums
3. Customer Notification Cost
4. Brand Damage
5. Potential Lawsuits

Why traditional resiliency solutions won’t protect you from logical data corruption

	You have	What is required
Replication	Data is being replicated continuously but logical errors are also replicated instantaneously	Scheduled point in time copies stored in an isolated, secure location
Error detection	Immediate detection of system and application outages	Regular data analytics on point in time copies to validate data consistency
Recovery points	Single recovery point that likely will be compromised	Multiple recovery points
Isolation	All systems, storage and tape pools participate in the same logical system structure	Air gapped systems and storage so that logical errors and malicious intruders can not propagate
Recovery scope	Continuous availability and disaster recovery	Forensic, surgical or catastrophic recovery capabilities

What is an Immutable Copy?

An immutable copy is a backup file that can't be altered in any way. An immutable copy is unchangeable and able to be deployed to production servers immediately in case of malware, ransomware or wiperware attacks or other data loss.

Speed up the recovery from cyber attacks with Immutable copies

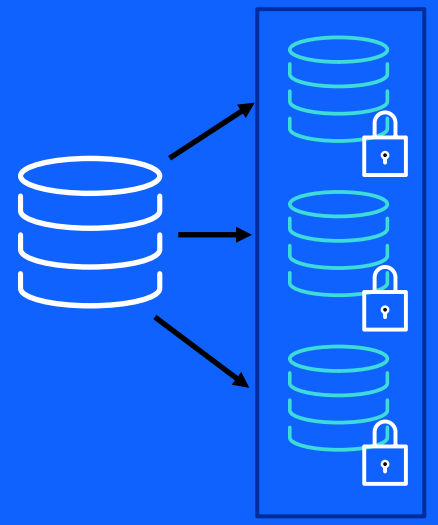
Automatic
creation of regular backup copies

Immutable/unchangeable
point-in-time copies of production data

Isolated
logical air-gap offline by design

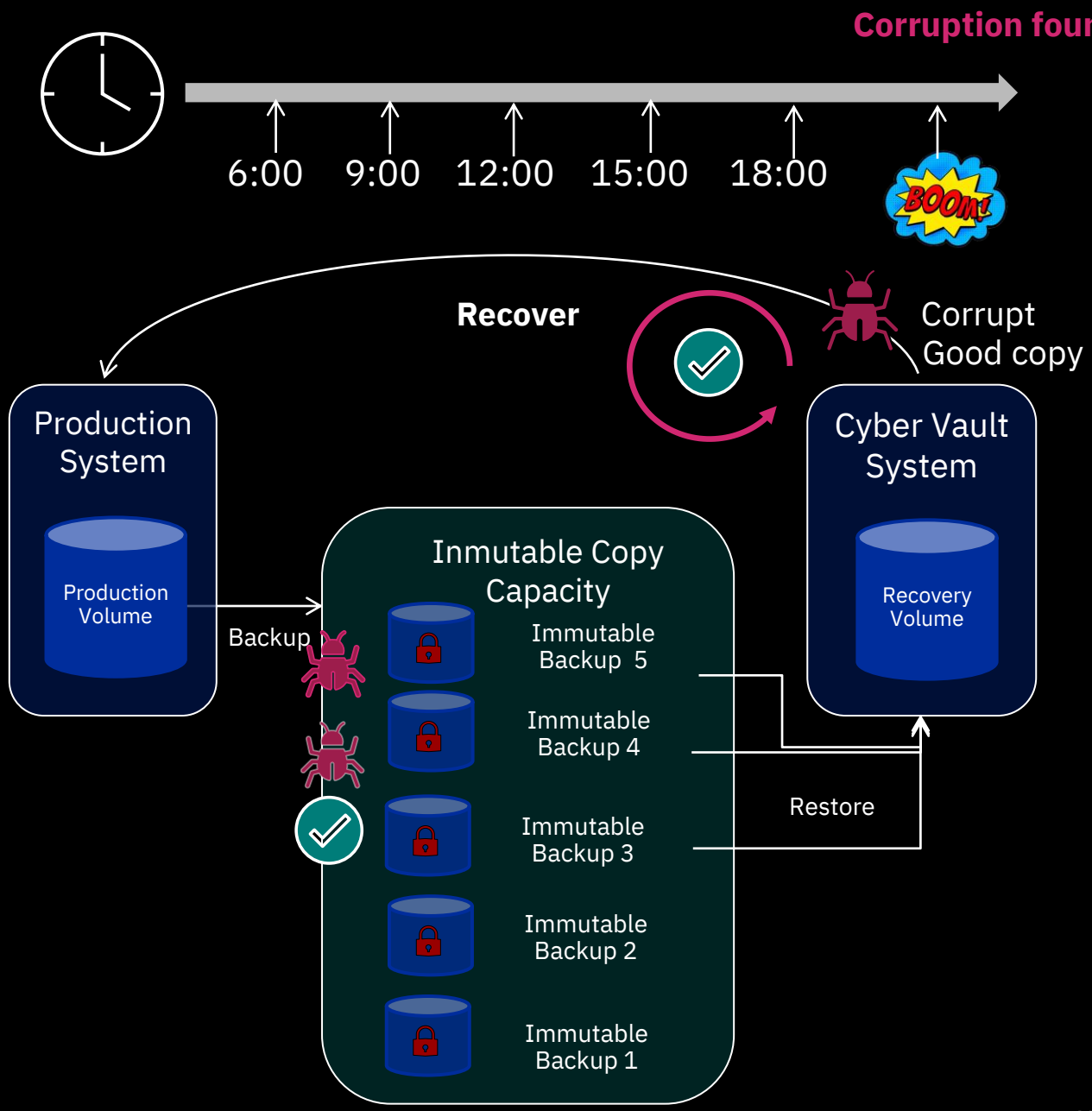
Fast
restore from copies on primary storage

Prevents modification or deletion of copies due to user error, malicious destruction, or ransomware attack



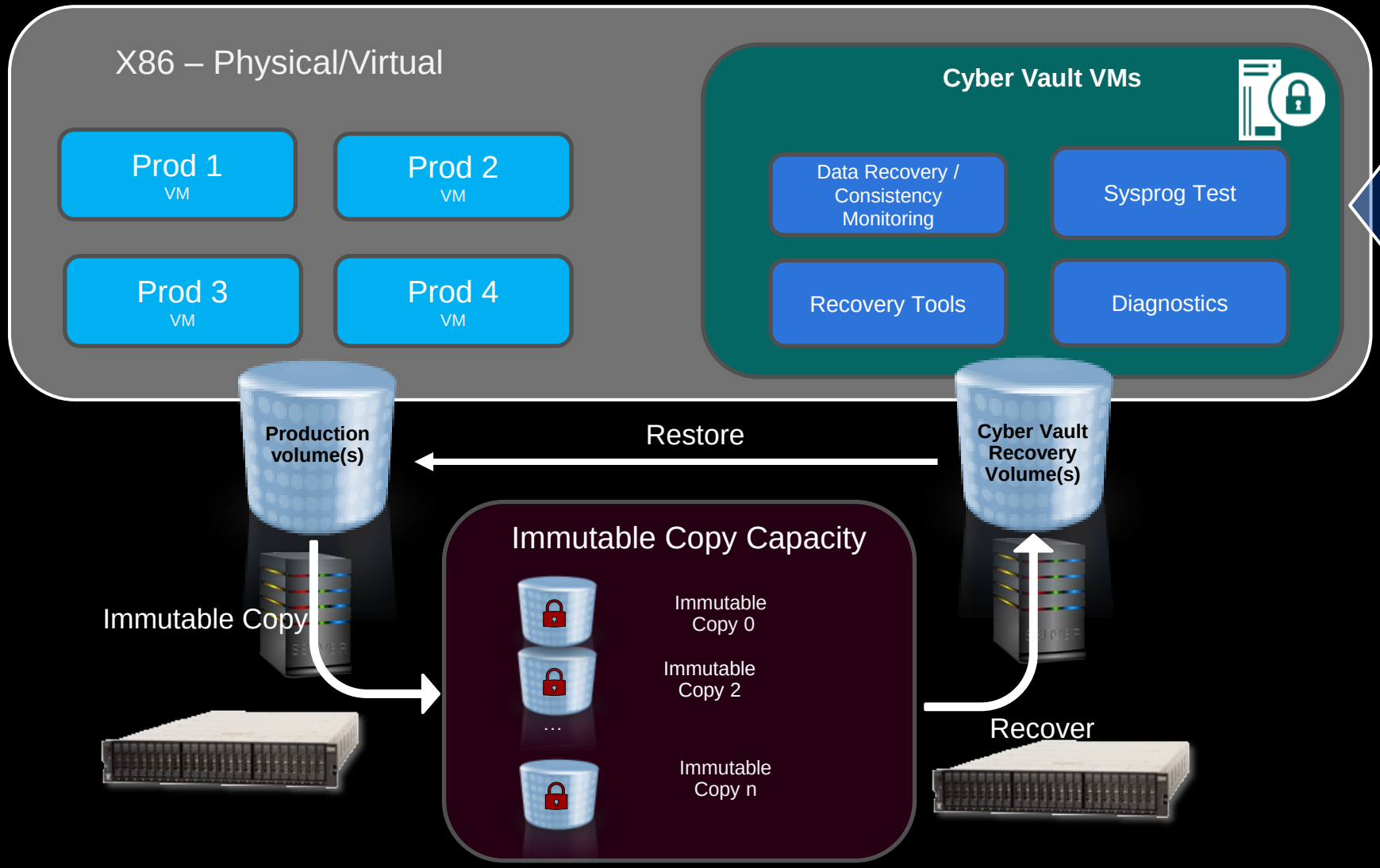
Immutable Copies Provide

- **Logical Corruption Protection** to prevent sensitive point in time copies of data from being modified or deleted due to errors, destruction or ransomware
- Data is accessible *only* after immutable copies are **recovered to a separate recovery volume**.
- **Proactive monitoring** for signs of attack
  - Identify Safe Volume to recover based on time index of identified attack
- Recovery volumes are used for:
  - Data validation
  - Forensic analysis
  - Restoration of production data



Consistency monitoring, analytics, and testing

Identify problems and solutions faster, minimize recovery impacts

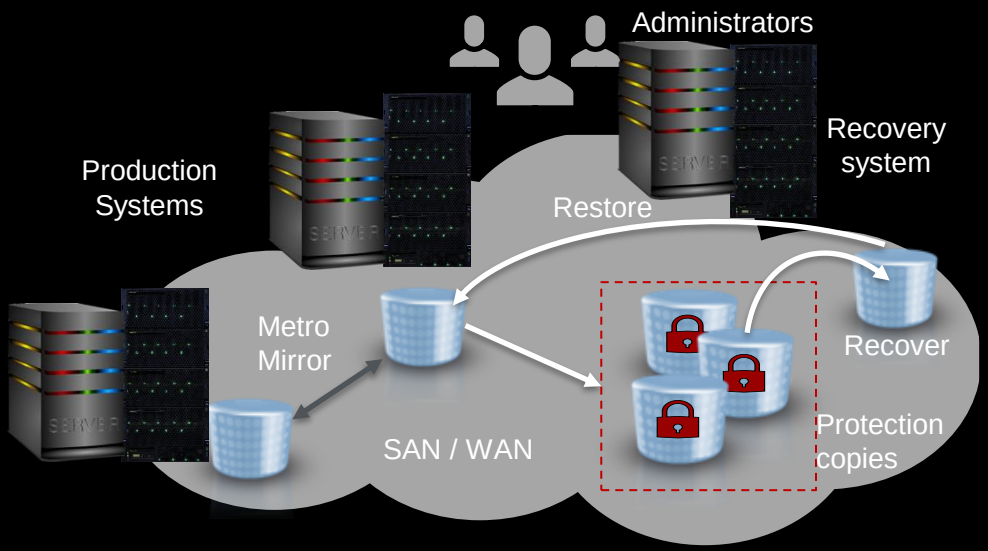


Cyber Vault Server/VMs

1. Establish analysis environment
2. Run diagnostic tools
3. Determine data validity

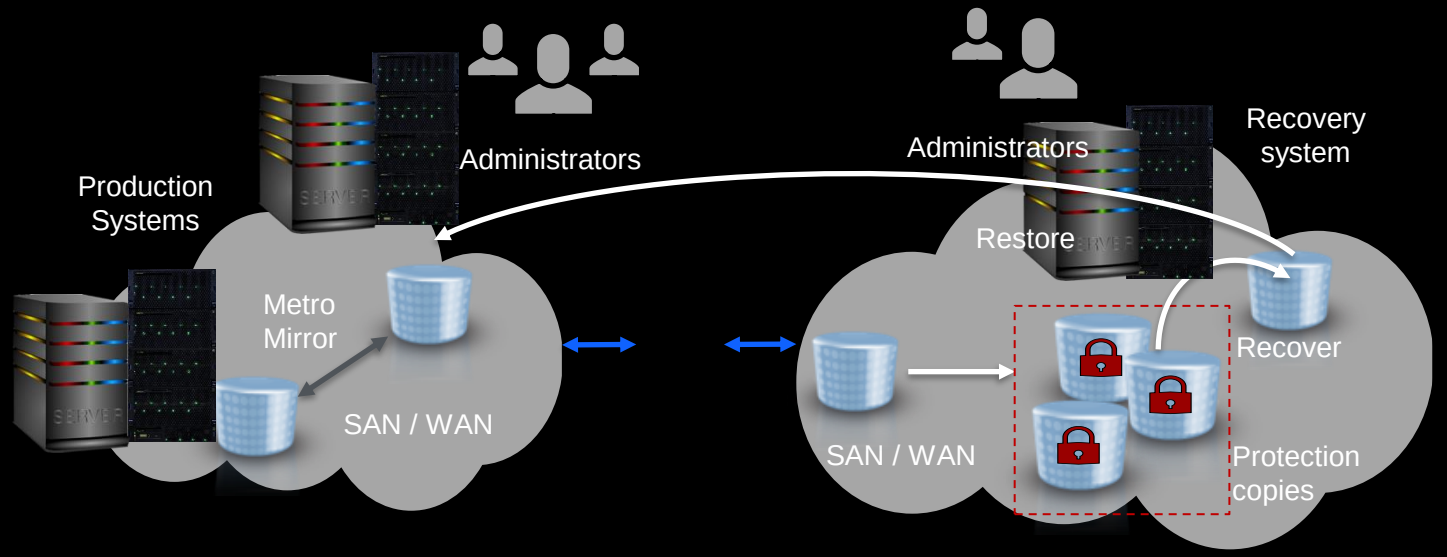
Air gap: Virtual and physical isolation of protection copies

Virtual isolation



- The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- The storage systems are typically in the same SAN or IP network as the production environment

Physical isolation



- Air gapped solution
- Additional storage systems are used for the protection copies
- The storage systems are typically not on the same SAN or IP network as the production environment
- The storage systems have restricted access and even different administrators to provide separation of duties

3 Step Process to Protect Your Data

1

Make immutable copies of data

- Immutable SNAP Shot Copies
- Automated creation and restore of copies

2

Test copies of data

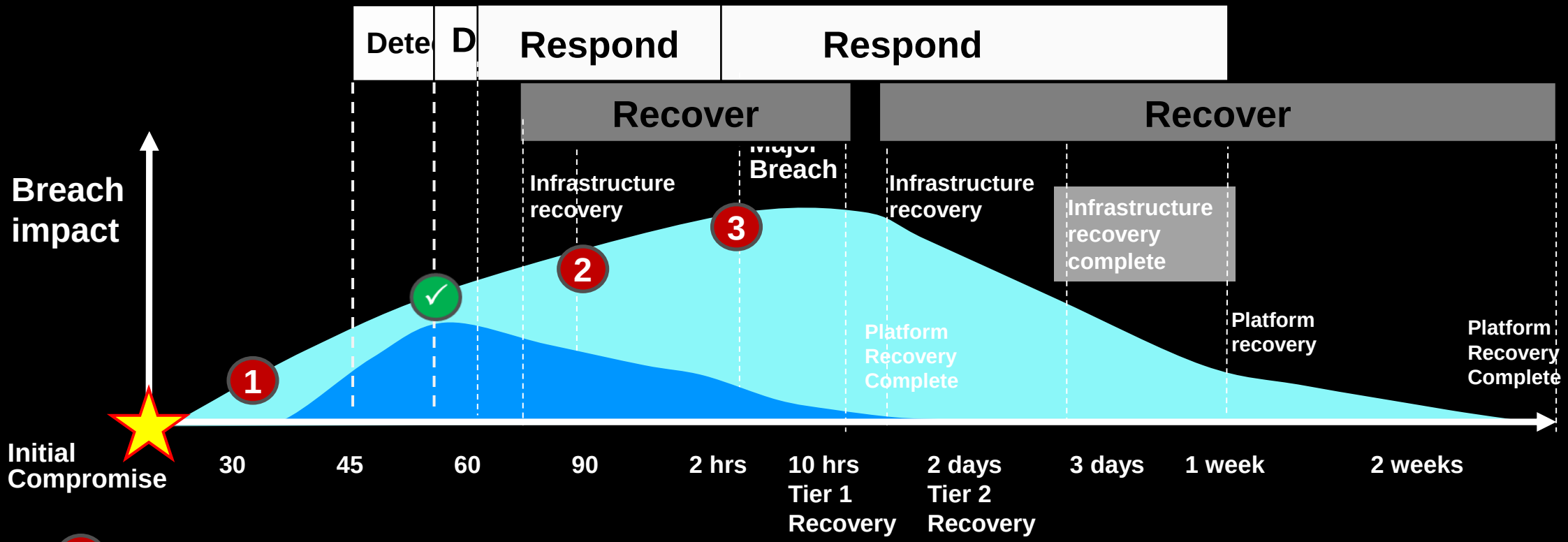
- Isolated infrastructure to test copies
- Ensure copies not corrupted using application tools
- Test infrastructure logically or physically air-gapped
- Blueprint for testing and recovery process

3

Automate process

- Automation of making and testing copies
- Automation of test & restore process

Cyber attack detection and recovery



1. Corruption of data occurs - but not yet detected
2. Without immutable copies and Data Resilient implementation corruption is detected much later and has a greater chance to spread
3. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

✓ Due to Immutable copies and the use of the Data Resilient implementation, data is continuously checked and corruption is found and corrected EARLIER & FASTER

Look at what else is needed, if anything?

What do we need?

We need tooling/solutions that:

- Detect potential attacks as early as possible; even using technology as AI and ML for behavioural analysis
- Identify at the database/file and even member level what has changed and when
- Ability to know what the last good version of the data was and where it's backed up
- Automation to generate the recovery points required to facilitate a surgical recovery

Enterprise-grade cyber security and resiliency

Data validation
Detect data corruption early or certify that the copy is clear

Forensic analysis
Investigate the problem, determine the best recovery action

Surgical recovery
Extract data from the copy and logically restore back to production environment

Catastrophic recovery
Recover the entire environment back to a point in time copy

Offline backup
Backup copy of the clean environment to offline tape media

Oracle tools such as DBVerify, backup tools to validate checksum or run with db_checksum

Db2 tools such as Db2 inspect and db2dart

SQL Server tools such as checkdb or checktable

MongoDB tools – backups and oplog forward recovery

Warehouse databases – Typical to have a set of validation SQL that is run against the tables after each load job and use the output of that SQL against the live dbase to validate that the data in the tables was still good

SIEM Tools, Data Analytic Tools

Index Engines CyberSense

Typical Current Environment

Immutable Copies of Data

Most Don’t have this
Maybe Air Gap “Traditional Backup” based solution

Proactive Monitoring

Almost all have a SIEM

Data Resiliency

Methodology & Automation

Rapid Recovery

MOST can NOT do this

Data Copy Test and Validation

Many have application based scanning tools
e.g. DBA manage scanning and recovery of DB

You Will Need A Cyber Resilience Strategy

An effective cyber resilience strategy relies on several operational activities:

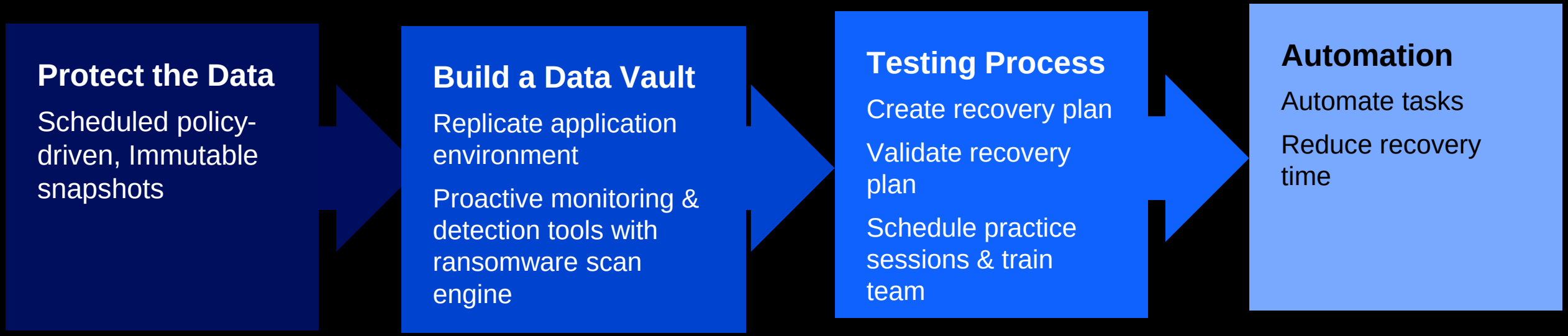
- Business continuity (BC)
- Disaster recovery (DR)
- Incident Response (IR)
- Cybersecurity Planning/Plans

The goal is to ensure the organization can resume operations as soon as possible in the aftermath of a ***successful*** cyber attack

In practice, the above elements usually exist in silos

A successful cyber resilience plan depends on understanding the interrelationships among these parts and how each component complements the functions of the others

Roadmap to achieving Cyber Resiliency



“Continue The Journey”

Cyber Resiliency

Thank You For Your Time

Peter D. Bille – Storage Solution Specialist
Pdbille@ibm.com